

CLAIMS

What is claimed is:

1. A generator of random numbers by a flip-flop, having a data input to receive a first signal at a first frequency comprised in a predetermined range and an instantaneous value of which is conditioned by a disturbing signal, and having a clock input to receive a second signal at a second predetermined frequency, smaller than the first one, said second signal passing through a delay element giving the second signal a delay greater than or equal to a maximum period of the first signal.
2. The generator of claim 1 wherein said disturbing signal is provided by a third oscillator at an intermediary frequency between said first and second frequencies.
3. The generator of claim 1, further comprising a comparator to set up the first signal provided by a first oscillator before arrival on the data input of the flip-flop.
4. The generator of claim 1 wherein the first signal is provided by a first oscillator comprising a voltage-controlled oscillator having a control input to receive said disturbing signal.
5. The generator of claim 1 wherein the second frequency is selected to have a ratio of at least 100 with respect to a minimum frequency of the first signal.
6. The generator of claim 2 wherein the intermediary frequency is selected to have a ratio ranging between 5 and 20 with respect to a minimum frequency of the first signal.

7. An apparatus to generate random numbers, the apparatus comprising:

- a circuit element having a first input terminal to receive a first signal having a first frequency and a second input terminal to receive a second signal having a second frequency smaller than the first frequency;
- a first signal generator coupled to the first input terminal of the circuit element to provide the first signal;
- a second signal generator coupled to the second input terminal of the circuit element to provide the second signal;
- a third signal generator coupled to the first signal generator to provide a third signal to control the first signal generator; and
- a delay element coupled to the second signal generator to provide a delay to the second signal that is at least equal to a maximum period of the first signal.

8. The apparatus of claim 7 wherein the third signal has a third frequency that is between the first and second frequencies.

9. The apparatus of claim 7 wherein the circuit element comprises a flip-flop, and wherein the first input terminal comprises a data terminal and the second input terminal comprises a clock terminal.

10. The apparatus of claim 7 wherein the third signal generator includes:

- a series connection of inverters;
- a capacitor coupled between an output terminal of a last inverter in the series and ground; and
- a feedback loop between the output terminal of the last inverter and an input terminal of a first inverter in the series.

11. The apparatus of claim 7 wherein the delay element includes a plurality of inverters connected in series.

12. The apparatus of claim 7 wherein the second signal generator includes:

a series connection of inverters;

a capacitor coupled between an output terminal of a first inverter in the series and ground; and

a feedback loop between an output terminal of a last inverter in the series and an input terminal of the first inverter.

13. The apparatus of claim 7, further comprising:

a comparator to shape the first signal, the comparator having an output terminal coupled to the first input terminal of the circuit element and having a non-inverting input terminal coupled to the first signal generator to receive the first signal; and

a resistive divider circuit having a node coupled to a capacitor and to an inverting input terminal of the comparator.

14. The apparatus of claim 7 wherein the first signal generator comprises a voltage-controlled oscillator.

15. A method to generate random numbers, the method comprising:

providing a first signal at a first frequency in a predetermined range as a data input of a flip-flop;

controlling an instantaneous frequency of the first signal;

providing a second signal at a second frequency smaller than the first frequency; and

delaying the second signal with a delay at least equal to a maximum period of the first signal and providing the delayed second signal as a clock input of the flip-flop.

16. The method of claim 15 wherein controlling the instantaneous frequency of the first signal includes providing a third signal having a third frequency that is between the first and second frequencies and using the third signal to control the instantaneous frequency of the first signal.

17. The method of claim 15, further comprising shaping the first signal prior to providing the first signal as the data input.

18. The method of claim 15, further comprising using noise associated with the first signal to mask noise associated with a third signal that controls the instantaneous frequency of the first signal.

19. A system for generating random numbers, the system comprising:
a means for providing a first signal at a first frequency in a predetermined range as a data input of a flip-flop;
a means for controlling an instantaneous frequency of the first signal;
a means for providing a second signal at a second frequency smaller than the first frequency; and
a means for delaying the second signal with a delay at least equal to a maximum period of the first signal and providing the delayed second signal as a clock input of the flip-flop.

20. The system of claim 19, further comprising a means for shaping the first signal.